



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,081	11/16/2001	David Rogoff	45620/JEJ/B600	1176
23363	7590	04/07/2006	EXAMINER	
CHRISTIE, PARKER & HALE, LLP			DINH, MINH	
PO BOX 7068			ART UNIT	
PASADENA, CA 91109-7068			PAPER NUMBER	
			2132	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/991,081	Applicant(s) ROGOFF ET AL.	
	Examiner Minh Dinh	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 January 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-15,23-26,30-32,37,38 and 41-44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-15,23-26,30-32,37,38 and 41-44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 November 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>1/20/06</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 01/20/2006. Claims 23 and 37 have been amended; claims 16-22, 27-29, 33-36 and 39-40 have been cancelled; claims 41-44 have been added. The specification has also been amended.

Response to Arguments

2. Applicant's arguments filed 01/20/2006 have been fully considered but they are not persuasive. Applicant argues that Davis disclose "a key source for storing a cryptographic key, encrypting the cryptographic key" or "a transmitter for receiving the digital data, receiving the encrypted cryptographic key over the control bus, decrypting the encrypted cryptographic key to recover the cryptographic key" (page 10, 3rd paragraph). Davis discloses method for distributing a cryptographic key from a cryptographic unit (fig. 4, element 335) to a chipset (fig. 4, element 315) wherein the cryptographic unit has a file key, encrypts the file key using a message key shared between the cryptographic unit and the chipset, and transmits the encrypted file key to the chipset; and the chipset receives data to be encrypted, receives the encrypted file key and decrypts the

encrypted file key using the message key to recover the file key (col. 6, lines 9-35).

Applicant argues that Davis does not disclose the limitations of claims 2-3 and 6-7 (page 10, last paragraph). With respect to claim 2, Davis discloses that the cryptographic unit generates the file key; inherently, the generated file key is first stored either in some register or in the volatile memory element of the cryptographic unit (fig. 4, element 615). Davis also discloses that the shared message key is stored in a second memory (fig. 4, element 610) and that the cryptographic unit encrypts the file key using the shared message key (col. 6, lines 25-28). With respect to claims 3 and 6-7, Davis discloses that the chipset decrypts the encrypted file key using the shared/symmetric message key to recover the file key (col. 6, lines 25-35) and that a conventional cryptographic algorithm such as DES is used (col. 3, lines 33-36).

3. Applicant's arguments with respect to claims 23-26 and 37-38 have been considered but are not persuasive. Applicant's amendments have necessitated a new search and new grounds of rejection.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-4, 6-7, 10-14 and 30-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis (5,818,939). Davis discloses a system comprising: a key source for storing a cryptographic key, encrypting the cryptographic key, and for transmitting the encrypted cryptographic key over a control bus (fig. 4, elements 330, 335; fig. 8); and a transmitter for receiving the digital data, receiving the encrypted cryptographic key over the control bus, decrypting the encrypted cryptographic key to recover the cryptographic key, encrypting the digital data using the cryptographic key to generate encrypted data, and for transmitting the encrypted data (fig. 4, element 315; fig. 8; col. 3, lines 21-45).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis as applied to claim 1 above, and further in view of "Philips Semiconductors Increases I2C-Bus Speed to 3.4 Mbits Per Second; New High-Speed Mode Targeted for Fast, Mixed-Voltage Systems" (hereinafter "Philips Semiconductors"). Davis does not disclose using an I²C bus. "Philips Semiconductors" discloses using I²C bus (Abstract). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis system to use an I²C bus, as taught in "Philips Semiconductors". The motivation for doing so would have been to provide an ideal solution for today's high-speed, mixed-voltage systems.

8. Claims 8-9 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis as applied to claim 1 above, and further in view of Saito (6,789,197).

Regarding claims 8, Davis does not disclose using a public key system. Saito discloses using a public key system (col. 3, lines 4-16). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis system to use a public key system, as taught by

Saito. The motivation for doing so would have been that it would be very difficult to cryptanalyze the crypton.

Regarding claims 9, Saito does not disclose using the RSA algorithm for the public key system. However, Examiner takes Official Notice that the RSA algorithm is a de facto standard and using the RSA algorithm is well known in the art. It would have been obvious at the time of the invention was made to modify the combined system of Davis and Saito further to use the RSA algorithm because it is a de facto standard.

Regarding claim 15, Davis does not disclose that the system is utilized as a set-top box. Saito discloses a similar system that is incorporated into a set-top box to provide data copyright management function (Abstract, figure 3). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Davis system into a set-top box, as taught by Saito, so that the system could be used to provide data copyright management function.

9. Claims 23-26, 37-38, 42 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Komuro et al (WO 99/22372) in view of Silicon Image ("High-bandwidth Digital Content Protection – White Paper").

Komuro discloses a system comprising: a key source comprising a set-top box for storing a cryptographic key, encrypting the cryptographic key, and

for transmitting the encrypted cryptographic key over a communications link (figure 5A, elements 120' and 125; figure 7), the communications link being functionally equivalent to a control bus linking two separate devices (Specification, page 26, line 30 – page 27, line 13); and a receiver comprising a digital TV for receiving the encrypted data, receiving the encrypted cryptographic key over the control bus, decrypting the encrypted cryptographic key to recover the cryptographic key, decrypting the encrypted data using the cryptographic key to generate digital data, transmitting the digital data and/or displaying the digital data (figure 5A, elements 120' and 125; figure 7; page 17, lines 1-6). Komuro does not disclose utilizing DVI interface for communication over I²C bus. Silicon Image discloses using DVI interface for communication over I²C bus (page 4, What is the Digital Visual Interface; page 10, figure 4 and 2nd paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Komuro system to utilize DVI interface for communication over I²C bus, as taught by Silicon Image. DVI interface provides a low-cost, high-speed digital link.

10. Claims 41 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Silicon Image. Davis discloses a system comprising: a key source for storing a cryptographic key, encrypting the

cryptographic key, and for transmitting the encrypted cryptographic key over a control bus (fig. 4, elements 330, 335; fig. 8); and a transmitter for receiving the digital data, receiving the encrypted cryptographic key over the control bus, decrypting the encrypted cryptographic key to recover the cryptographic key, encrypting the digital data using the cryptographic key to generate encrypted data, and for transmitting the encrypted data (fig. 4, element 315; fig. 8; col. 3, lines 21-45). Davis does not disclose utilizing DVI interface for communication over I²C bus. Silicon Image discloses using DVI interface for communication over I²C bus (page 4, What is the Digital Visual Interface; page 10, figure 4 and 2nd paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis system to utilize DVI interface for communication over I²C bus, as taught by Silicon Image. DVI interface provides a low-cost, high-speed digital link.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

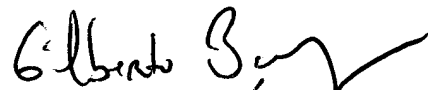
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
3/31/06



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100